



29 September 2021

Matt Brown
fyi-request-16225-9cbd5e80@requests.fyi.org.nz

REF: IR-01-21-23305

Dear Matt

I refer to your Official Information Act 1982 (OIA) request dated 27 July 2021 for information relating to Automatic Number Plate Recognition (ANPR) cameras.

I can provide the following response to your questions.

The number of ANPR cameras in-use or accessible (e.g. capable of generating a notification to NZ Police) by the NZ Police at the current time?

Police currently owns 18 mobile ANPR cameras that are deployed in vehicles. In addition, Police receives notifications from networks of third-party cameras. Police does not hold data on the number of ANPR cameras owned or operated by third-party networks.

A copy of the applicable Police operational policies (or equivalent documents) covering the criteria or situations in which ANPR cameras are judged suitable for use, and/or are prohibited from use.

The current Police manual for the operation of the ANPR devices which are possessed/operated by the New Zealand Police is enclosed. Please see attachment '*Automated Number Plate Recognition.pdf*'. This manual is undergoing a review and update process which will involve consultation with the Office of the Privacy Commissioner.

A copy of the Privacy Impact Assessment (or equivalent documents) covering NZ Police use of ANPR technology.

A Privacy Impact Assessment (PIA) was completed in August 2017. The full document is withheld under section 9(2)(g)(i) of the OIA, to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers



NEW ZEALAND
POLICE
Ngā Pirihimana o Aotearoa

and employees of any public service agency or organisation in the course of their duty. However, the executive summary of this PIA can be provided and you will find a copy enclosed. Please note information from this document has been withheld under section 9(2)(g)(i) of the OIA.

I trust this response is of use to you. You have the right, under section 28(3) of the OIA, to ask the Ombudsman to review my decision if you are not satisfied with the way I have responded to your request.

Yours sincerely

D.C. LYNCH
Detective Superintendent
New Zealand Police



**Police
Instructions**

Automatic Number Plate Recognition

Table of Contents

Table of Contents	2
Executive summary	4
Overview	5
Introduction	5
ANPR equipment	6
Components	6
Software	6
Servicing	6
ANPR vehicles	6
Training	6
Roles and responsibilities	7
ANPR operations - approved deployment models	8
Pre-deployment procedures	9
All deployment types	9
Limited scale deployments	9
Checkpoints	9
Mobile deployments	9
Non-standard deployments	10
ANPR deployment site plan examples	11
Generic examples	11
Parked deployment	11
Car park deployment	11
ANPR checkpoint	12
Selecting a location	13
Points to consider	13
ANPR checkpoint procedure	14
Radio procedures	14
ANPR equipment setup	14
ANPR checkpoint setup	14
VOI alerts - ANPR operators	14
Plate misreads	14
Multiple VOI alerts	14
Power to stop	15
VOI alert - intercept team	15
Approaching the driver	15
Acting on the alert	15
Following the stop	15
Access to and retention of ANPR data	17
VOI data entered into ANPR	17
Data obtained from ANPR deployments	17
Conditions of use	18
Removal of ANPR data from database	18
Privacy Act implications	18

Examples of proper use of the ANPR database

18

Examples of improper use of the ANPR database

18

Executive summary

The purpose of the Automatic Number Plate Recognition (ANPR) chapter is to ensure staff maximise enforcement opportunities, as a result of preloaded alerts, and use the tool in accordance with policy and legislation.

Key, critical points for staff to note:

- Only approved ANPR deployment methods and equipment are to be used.
- ANPR equipment must only be operated by Police who have completed formal training.
- Data obtained from ANPR deployments must only be retained for 48 hours.
- The ANPR system is only as effective as the data quality relating to the alerts - staff should correct and update any discrepancies.

Overview

Introduction

Automatic Number Plate Recognition (ANPR) is a technology used to automatically identify vehicles of interest (VOI), as flagged in the National Intelligence Application (NIA), Motor Vehicle Register (MVR), and Driver Licence Register (DLR), from their number plates.

The ANPR system uses optical character recognition (OCR) to scan vehicle number plates and check them against VOI alerts. In simple terms it assists officers by negating the need to refer to lists of VOIs by informing them when such a vehicle is detected by the system. When a VOI is recognised, the system alerts the operator who can take appropriate action.

The ANPR system allows officers to enhance enforcement opportunities by focusing on high risk drivers and offenders, ie, drink drivers, unlicensed drivers and persons with warrants who are linked to a VOI.

This document sets out:

- an overview of ANPR equipment;
- approved methods of deployment; and
- the procedures to be followed during the deployment of ANPR.

Note: This chapter applies to Police constables and authorised officers, hereafter referred to collectively as 'Police'.

ANPR equipment

Components

ANPR systems are made up of these components:

- a camera;
- a computer; and
- a monitor.

Software

ANPR systems use software which has limited support from the Police Information and Communication Technology (CT) helpdesk. Instructions on software operation and support contacts are included in the training given to ANPR operators.

Servicing

Instructions on software and hardware servicing are included in the ANPR operator manual.

ANPR vehicles

ANPR equipment must only be operated in purpose built ANPR vehicles in accordance with this Police Manual chapter. If it is operationally necessary to alter the vehicle or operate ANPR in any other manner, pre-approval must be gained from the Director: Road Policing prior to any change being made or organised - refer to the '[Police vehicle management](#)' chapter.

Training

ANPR equipment must only be operated by Police who have completed formal training from Road Policing Support staff, or have received formal training from an employee in their district who has used ANPR, and is competent in its use. To ensure national consistency and quality of content and delivery, all training must:

- be approved by the Director: Road Policing; and
- comply with the quality assurance standards set by the Police Training Service Centre (TSC).

Roles and responsibilities

This table sets out the roles and responsibilities associated with ANPR equipment.

Role	Responsibilities
Director: Road Policing	<ul style="list-style-type: none"> • Must approve the ANPR training session content. • May approve (in writing) requests to operate ANPR in non-standard deployments or outside of these guidelines.
District Commanders	Must ensure Police are trained to operate ANPR equipment prior to authorising operational deployment.
Officer in charge of ANPR operations	Must ensure all operational deployments of ANPR: <ul style="list-style-type: none"> • have a trained ANPR operator; • are used in a manner that enhances road safety and enforcement opportunities; and • maintain business as usual.
ANPR operator	<ul style="list-style-type: none"> • Must have completed an ANPR training session. • Must have read and understood the ANPR operator manual.
ANPR vehicle	<ul style="list-style-type: none"> • Must not be altered except by prior written approval from the Director: Road Policing. • Vans must be used as a category D vehicle and not be used to transport or hold prisoners. • Marked patrol vehicles fitted with ANPR are still a category A vehicle.
Support vehicles	These must be category A or B patrol vehicles. They should be operated by gold classified drivers .
ANPR Intercept Team	Must be aware of their powers when acting on a VOI alert as identified by ANPR.

ANPR operations - approved deployment models

Download the ANPR operations - approved deployment models:


 [ANPR_operations_-_approved_deployment_models.doc](#)

59 KB

Pre-deployment procedures

All deployment types

Follow these steps for all deployment types.

Step	Action
1	Ensure appropriate Police resources are available to conduct the type of approved deployment:  ANPR_operations_-_approved_deployment_models.doc 59 KB
2	Conduct a briefing on Police roles, responsibilities and operational focus, ie, high-risk drivers.
3	Ensure the ANPR equipment is ready to operate. The ANPR van also requires the batteries to be checked.
4	Ensure the ANPR operator obtains an up-to-date begin-shift folder containing the latest alerts.
5	Ensure the ANPR camera is set-up correctly: <ul style="list-style-type: none"> • For static deployments, set up the ANPR vehicle ensuring it is legally and safely parked. The vehicle's position must not disrupt the normal flow of traffic. • For mobile deployments where cars may be parked, the vehicle's camera angles may be adjusted prior to arriving at the deployment location. <p>Note: Sometimes ANPR is best suited in the middle of the road, scanning both lanes (oncoming / away).</p>
6	Inform the Communication Centre (Comms) of the nature and location of the ANPR deployment.

Limited scale deployments

Follow these steps for limited scale deployments.

Step	Action
1	For mobile deployments, ensure the ANPR vehicle driver does not monitor the ANPR equipment while driving. If you are one-up, pull over before checking the VOI alert.

Checkpoints

Follow these steps for checkpoints.

Step	Action
1	Prepare a deployment plan including a site plan .
2	Ensure adequate signage and cones are available.
3	The ANPR operator must ensure the intercept vehicles and checkpoint Police are in position and ready prior to commencing a deployment.

Mobile deployments

Follow these steps for mobile deployments.

Step	Action
1	For mobile deployments, ensure the ANPR vehicle driver does not monitor the ANPR equipment while driving.

Non-standard deployments

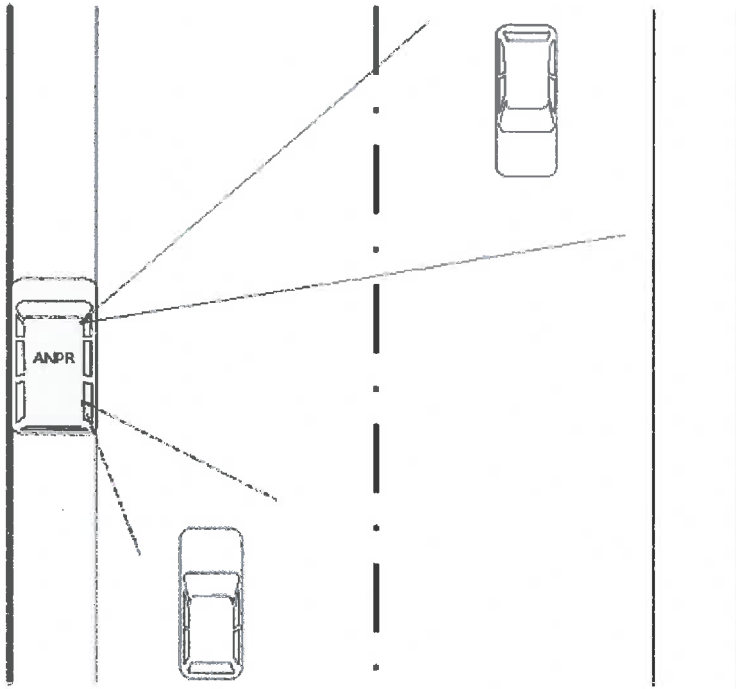
For non-standard deployments, such as Impairment Prevention Teams, comply with their standard operating procedures.

ANPR deployment site plan examples

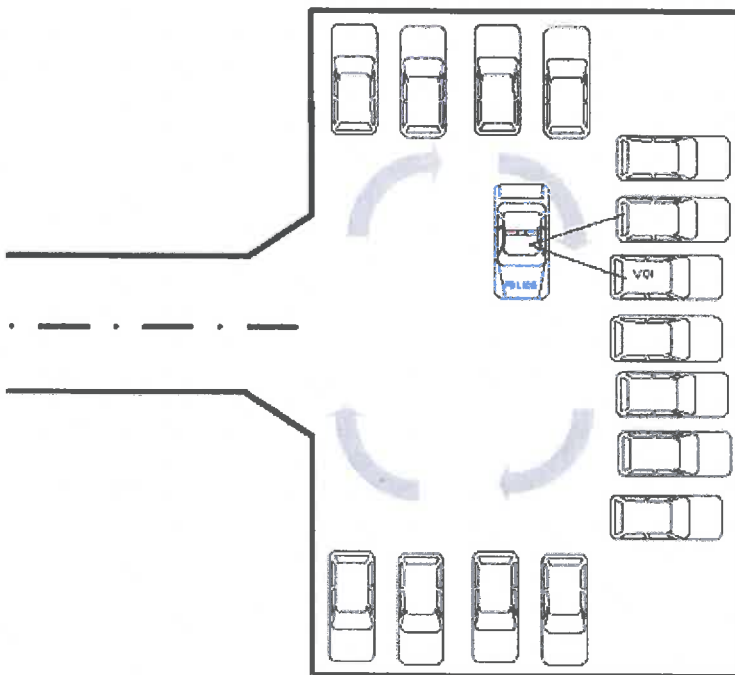
Generic examples

These are generic examples to assist the officer in charge of an ANPR operation with the preparation of site plans. For Impairment Prevention Team checkpoints refer to the ['Alcohol and drug impaired driving'](#) chapter.

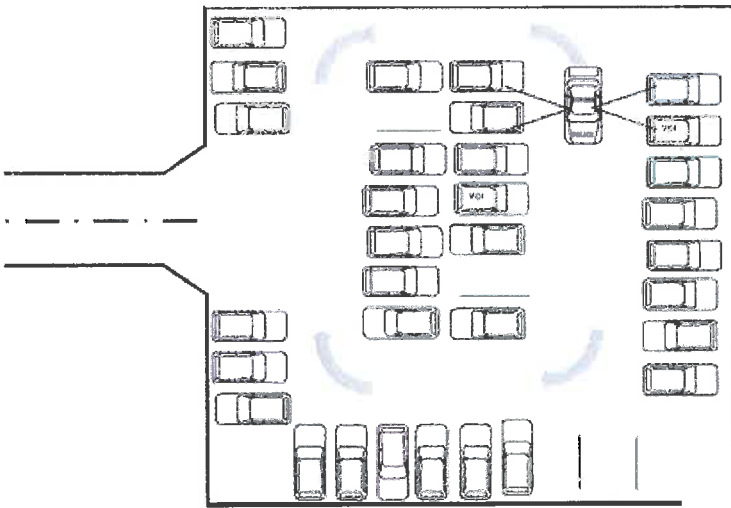
Parked deployment



Car park deployment

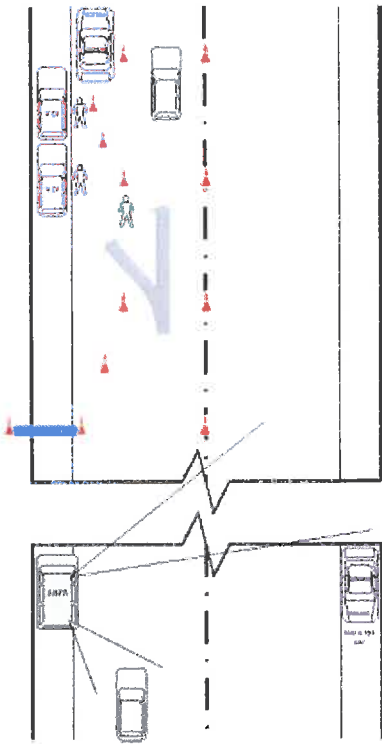


- Left parking mode -



- Dual parking mode -

ANPR checkpoint




- Single/dual traffic direction mode -

Note: The ANPR van/marked patrol vehicle can be set to read traffic in both directions where the checkpoint operates in both traffic directions.

Selecting a location

Points to consider

When selecting a location for all deployment types consider the Police Manual chapter [Perimeter control](#). For ANPR checkpoints also consider this table.

Consider	Rationale
The deployment model (see below)	Not all deployment models are suitable for all locations.
 ANPR_operations_-_approved_deployment_models.doc 59 KB	
Traffic volumes	To maximise the potential of ANPR, higher volumes of traffic are recommended. Only a small percentage of vehicles have VOI alerts.
Intercept risks	Consider deployment sites which allow easy migration of the ANPR or intercept vehicle into traffic flow and limit an offender's escape routes. Areas with side roads or additional potential for offenders to do u-turns increase intercept risks.
Officer/public safety	Avoid areas where drivers have little reaction time prior to arriving at a checkpoint, or there is a risk of nose-to-tail crashes if traffic begins to queue. Avoid areas with poor overhead lights at night.
Hazard creation	The ANPR vehicle should be legally parked and in a manner that ensures the operator's and public safety.
Service disruption	Avoid checkpoints that disrupt the flow of emergency service vehicles, e.g. near Police or fire stations. When operating with a Impairment Prevention Team ensure the ANPR intercept team operates behind the Impairment Prevention Team.
Sufficient room for the intercept team and vehicles	The intercept team needs enough space to safely process VOIs, including room to tow impounded vehicles.
Local knowledge	Police will know areas where successful operations have been conducted in the past.

ANPR checkpoint procedure

Radio procedures

Where possible, only use Mobility devices for communications to limit radio traffic. Follow these steps (not necessarily in the order shown here).

Step	Action
1	Ensure Comms are aware of the nature and location of the ANPR deployment and at least one member of the intercept team monitors the main radio channel.
2	Ensure support vehicle radios remain on the main radio channel so that communication is on the main channel if an offender fails to stop when signalled to do so. For further information refer to the 'Radio and Emergency Communication Centre Protocols' chapter.
3	Use a closed simplex channel for communication between the ANPR operator and intercept team. This channel should be kept free to allow the ANPR operators to broadcast the VOI alert type and description.

Note: The intercept team should only communicate to acknowledge the VOI alert or when they are all busy and do not require further alerts to be broadcast.

ANPR equipment setup

Refer to the ANPR Operator Manual.

ANPR checkpoint setup

Follow the [site plan](#) and for positions of the ANPR vehicle, support vehicles, signage and cones.

VOI alerts - ANPR operators

ANPR operators must follow the procedure in figure 1 below when a VOI is detected.

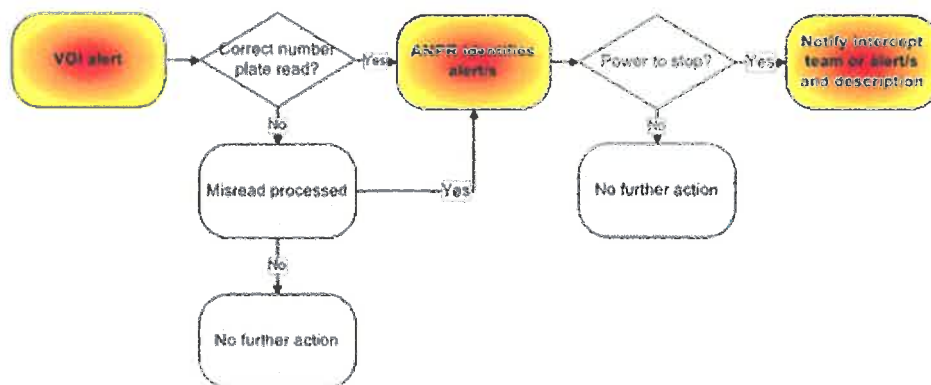


Figure 1: ANPR operators' decision chart

Plate misreads

The ANPR OCR software may occasionally misread similar shaped characters such as a '1' as an 'l', or an 'O' as a 'Q'. The ANPR operator must compare the photograph of the captured plate with the OCR definition to determine if the plate has been read correctly.

Multiple VOI alerts

The ANPR software does not prioritise VOI alerts in order of seriousness, where a detected vehicle has multiple VOI entries. Prior to informing an intercept team of VOI activity, all VOI alerts for the detected vehicle must be assessed and prioritised. The ANPR operator must ensure that the VOI information passed to the intercept team accurately reflects all information held on the detected vehicle. This enables the intercept team to assess the threat level and plan accordingly in accordance with 'TENR'.

Power to stop

New Zealand legislation provides Police with various powers to stop vehicles. However, Police do not have a blanket power to stop any vehicle except for the purpose of a [compulsory breath test](#). As a general rule:

- For alerts relating to the [Land Transport Act 1998](#) offences, section 114 applies.
- For alerts where the [Search & Surveillance Act 2012](#) applies, refer to sections 9 and 121.

Some NIA VOI alerts such as 'other' will require the ANPR officer to check the alert text to determine if a power to stop exists. For more information refer to:

- 'New Zealand Bill of Rights'
- 'Traffic patrol techniques'
- 'Perimeter control'.

VOI alert - intercept team

Once notified of the alert type and vehicle description, the intercept team can prepare to stop the vehicle. Depending on the alert type consider:

- the statutory obligations pursuant to the power to stop under the [Search & Surveillance Act 2012](#);
- the risk the driver may fail to stop; and
- the risk the driver or passengers may flee on foot.

For more information on stopping vehicles refer to: [Traffic patrol techniques](#)'.

If a vehicle fails to stop, follow the [Fleeing driver policy](#)' and '[Urgent duty driving](#)' policies. Intercept staff should be aware that a VOI, failing to stop on request, does not automatically provide sufficient grounds to pursue the fleeing vehicle.

Approaching the driver

For information on approaching the driver of a vehicle refer to: [Traffic patrol techniques](#)'.

Acting on the alert

Remember that some VOIs may no longer be of interest to Police but are yet to be expired. This must be considered when dealing with the driver.

For information on actions to be taken when acting on the alert refer to the appropriate Police Manual chapter. The main chapters are listed below:

- '[Alcohol and drug impaired driving](#)'
- '[Arrest and detention](#)'
- '[Driver licensing](#)'
- '[Impounding vehicles](#)'
- '[Issuing non-operation orders](#)'
- '[Motor vehicle offences](#)'
- '[Motor vehicle registration and licensing](#)'
- '[Motor vehicle noise enforcement](#)'
- '[Offence notices](#)'.

Following the stop

If it is necessary to do so, update or expire the NIA alert to reflect the current status of the vehicle or notify the agency responsible for the source data. Ensure that intelligence notings are submitted in a timely manner.

Access to and retention of ANPR data

VOI data entered into ANPR

VOI data consists of vehicle registration numbers which are of interest to Police or require enforcement action, eg, high risk drivers. As the VOI data is derived from different data sources it must be treated the same as NIA data in accordance with the policies and rules set out in the [NIA manual](#).

District intelligence units and operational groups are authorised to create NIA alerts, by linking high risk drivers or offenders to vehicles, in order to target specific problems.

NIA is under-utilised currently for the detection of POIs / VOIs, such as:

- High risk drivers,
- POIs with warrants to arrest, and
- POIs wanted for breach of bail.

By improving the linking of POIs to vehicles, improved detection and apprehension of POIs can be achieved for both ANPR, and during mobile QVRs.

Note: An appropriate expiry date must be entered against the alert in NIA.

Regardless of the alert entered onto NIA, expiry dates are critical to effective use of the ANPR vehicle and mobile queries. This is important as a POI may drive several vehicles. District intelligence units and operational groups must not create their own databases for use with ANPR.

VOI alerts which trigger the automated VOI extract file for ANPR are currently:

- Known to be driven by a disqualified driver
- Known to be driven under the influence of Drugs or Alcohol
- Driver Forbidden to Drive
- Non Op Order - Pink Sticker
- Non Op Order - Green Sticker
- Prohibition Notice s.248 LTA issued
- Wrecked - i.e. plates removed from vehicle for disposal
- Stolen vehicle alert
- Petrol Drive Off
- Other (specify - boy racer events)
- Person Safety Alert
- Organisation Safety Alert
- Sought
- Important Information.

VOI data from other Government agencies, eg, the New Zealand Transport Agency, may also be utilised in the ANPR system. This must only be data from agencies that have a written agreement with Police to share data for the purposes of ANPR deployments.

Data obtained from ANPR deployments

Data obtained from deployments will only be retained for 48 hours.

The data obtained from ANPR deployments consists of:

- a list of registrations captured by the ANPR camera;

- an image of a registration plate; and
- an image of part or all of the vehicle (depending on how the camera is set up).

At the end of every shift, the ANPR operator must:

- upload data from the ANPR system to a secure USB flash drive ('Ironkey'); and
- on return to their Police station, transfer the data to the BOSS system. The data may be manually processed and deleted, or the BOSS system will automatically delete the data after 48 hours.

All ANPR data retained for processing must only be stored in the J:Drive, ANPROVI folder, Endshift folder, and into your respective districts folder. If records are in excess of 48 hours old and the software is activated, the system will automatically delete the data.

If you have access to BOSS Server, download the Iron-Key directly onto the standalone BOSS laptop by completing a synchronisation.

The data will be of no use if it is processed after 48 hours from the time the read or hit was obtained, as BOSS automatically deletes the information after this period.

Conditions of use

The underlying principle governing the proper use of the ANPR database is it must be used for Police business purposes only. Refer to the information on Police computers section in the ['Information security'](#) chapter in the Police Manual chapter.

Removal of ANPR data from database

All data obtained from ANPR deployments automatically drops off the BOSS system after 48 hours.

Privacy Act implications

Collection of personal information (number plates) using ANPR has implications under the Privacy Act 2020. To ensure Privacy Act compliance, it is important that the procedures in these instructions are followed. In particular:

- ANPR must only be used where it is necessary for a lawful purpose connected to a Police function. In this case, the purpose is identification of high risk drivers and offenders to enhance enforcement opportunities.
- The information that is collected must be stored securely, and not retained for longer than necessary.

ANPR data from the database must not be circulated or disclosed to any other Government or third-party organisation or person without the express authorisation from the Commissioner, or another officer delegated by the Commissioner to give such authorisation.

Examples of proper use of the ANPR database

ANPR data may be used as an investigative tool for the purposes listed in this table. The table also provides examples of proper use.

Purpose	Example of proper use
Locate an offender	A constable may stop a vehicle that is linked to an offender requiring further Police action.
Locate lost or stolen vehicles	<ul style="list-style-type: none"> • A vehicle is reported stolen and Police create an alert in NIA. • A vehicle identified as part of a deployment may be stopped; or • a constable could check the previous 48 hours of ANPR deployment records to determine if the vehicle's movements can be determined to assist in its location and recovery.
High risk drivers	A constable may intercept a vehicle that is linked to a high risk driver, i.e., recidivist drink driver or person with a warrant to arrest.

Examples of improper use of the ANPR database


ANPR data must be used in connection with a lawful Police activity. Using data in the absence of a law enforcement purpose will constitute a breach of the [Privacy Act 2020](#).

ANPR data should not be used...	Example of improper use
in situations where Police attend peaceful protests or meetings where members of the public are exercising their right to freedom of expression.	A constable is supervising a peaceful public meeting. S/he uses the ANPR camera to record the registration numbers of all the vehicles travelling to the venue. S/he knows the vehicles are unlikely to be VOIs but plans to check the captured number plates in NIA to determine the names and addresses of the meeting attendees.
to monitor the movements of a person in the absence of any suspected unlawful activity.	A constable observes a person they would like to meet socially driving a vehicle and makes a note of the vehicle's registration plate. The constable checks the ANPR database to determine the vehicle's movements in the hope of being able to meet that person.
for the purposes of political, commercial, or financial gain.	In addition to being a Police employee, a constable owns a business with her/his partner. The constable learns that a representative of a rival company is in the local area. S/he knows the details of the vehicle the representative is driving and checks the ANPR database to monitor the movements of that vehicle.

If a Police employee is uncertain whether ANPR data is being used legitimately, they must discuss the matter with their supervisor.

Printed on : 28/05/2021

Printed from : <https://tenone.police.govt.nz/pi/automatic-number-plate-recognition>



Automatic Number Plate Recognition – Privacy Impact Assessment

Abstract: A review of the Counties Manukau Project to acquire and use Number Plate Information (NPI) from private Automatic Number Plate Recognition (ANPR) platforms

2.0 Executive summary

2.1 – The Project

The Project is an endeavour by the Counties Manukau District to acquire data about motor vehicles from existing privately operated (non-police) CCTV systems using ANPR software. The NPI data will be stored and available in a database known as the Vehicle Identification Broadcast Engine (VIBE), supplied by SecuroGroup, a private software company.

There is a growing use of ANPR private operators. ANPR software has become more affordable and effective. Groups of retailers, owners of large car parking complexes and local authorities are all tapping into the security benefits of the tool. Government entities such as NZTA are exploring the possibility of using ANPR for roading use intelligence. Figures on how many ANPR platforms there might be New Zealand wide are not available. Auckland Police continue to be approached by Community Partners wanting to provide NPI to Police. It is a safe assumption that if this project were to become a nationally owned crime tool in the future, the potential number ANPR sites connected to Police could be significant.

Recent information suggested that in the Northland region there are 3 Northland towns keen to supply NPI data, their contribution arising from up to 700 cameras. It is a safe assumption that nationally the potential ANPR platforms number in the many 1000s.

ANPR ought to be viewed as a forerunner to the wider use of other CCTV platform options such as 'facial recognition'. Already another Police district is contemplating the opportunity provided by retailers who have deployed 'facial recognition' software.

The United Kingdom experience, which is significantly saturated, is a useful case study on appropriate/inappropriate use of NPI. Unlike the VIBE project at hand, the UK Government/Police Forces actively funded the installation of thousands of new ANPR cameras. It now owns and operate over 8000 CCTV/ANPR platforms and acquires 10s of millions of lines of data on a daily basis⁶. Their journey to acceptable use of NPI included a significant public furore, new legislation governing the use of CCTV, the appointment of a Surveillance Camera Commissioner and the creation of a Home Office National ANPR Data Centre. In addition the legislation created a Surveillance Camera Code of Conduct. By all accounts this was a substantial and lengthy process.

There will be much to learn from the UK Police experience and tapping into that experience would be valuable to NZ Police, to assist with the responsible uptake and use of NPI.

In addition to the UK experience, cognisance of the current social climate in New Zealand is important. Section 9(2)(g)(i)

The public debate has drawn in concerns about the security and use of data in the Integrated Data Infrastructure (IDI) administered by Statistics NZ. The public perception is that the State sector is not a trusted steward of citizen's sensitive data.

Without a strong corporate strategy around VIBE, Police acquisition of private NPI data could be characterised as 'mass surveillance' or 'big brother' behaviour. Careful thought and assurance needs be given to the introduction of how the Project is managed, deployed and operated. There is good potential for positive exposure and community benefit from this project. Section 9(2)(g)(i)

Current features of concern with the project include;

2.2 Collection of NPI

There is a need for a defensible and thoughtful *purpose* for collecting NPI. That purpose ought to be supported by research about the utility, necessity and proportionality of using NPI for crime detection. In addition it is desirable that the Project is publicly introduced in a transparent manner by briefing the Minister of Police and the Privacy Commissioner.

⁶ Professional Police Magazine: Future of ANPR, p16 1/12/2016

2.3 Security

Security in a project involving technology and personal information has to be wider than just database and technical security. The considerations around guidance and policy, and physical access to the system and structural security must be connected and complimentary. Being able to determine access and behaviour within the system by any individual is important.

The Project also involves 3rd parties who engage with Police in various ways. SecuroGroup and the Fusion Data Centre both supply the technical capability for Police to hold, store and use NPI. They are agents of Police who should operate at a secure and responsible level commensurate with Police's own expectations of itself.

This concept also extends to those parties who are happy to supply NPI from their systems for Police use. They will be seen by the public as acting in tandem or as agents of Police. They will all be using the same NPI data to which Police has access. Having common expectations of this cohort of 3rd parties about their level of security around their systems, their uses of the data and their audit capacity are matters that Police should be assessing, before receiving data from them.

2.4 Use of personal information

How NPI will be used and for what is unclear. Linked to the overall purpose of why Police will acquire NPI, clarity around the rules and limits on the use of it are crucial to the integrity of the Project. The thinking about use in general ought to consider the need for limits on disclosure as well.

2.5 Retention of Personal Information

The Project's current thinking about retention periods for NPI data is arbitrary at best. If NPI was to be used simply to detect stolen vehicles in real time, very short periods of retention would be expected. By extending the purpose and use of NPI to include detection of crime, longer periods of retention are potentially defensible. More thought is required about the rationale for stated retention periods.

2.6 Governance and Assurance

In light of the Project potentially becoming a national application, adequate governance and robust assurance are prerequisites for the integrity of the practice. A high level governance group working in tandem with a knowledgeable working group, and a robust '3 lines of defence' model of assurance, perhaps with a 3rd line of defence that includes some external independent oversight are very important attributes for the Project. The governance and assurance should be managed from a central executive perspective.

Recommendations

<p>Collection of NPI</p>	<p>Formulate a defensible 'purpose' for collecting ANPR</p> <p>Conduct research that demonstrates the utility and public benefit of Police use of ANPR for stolen vehicles and crime in general</p> <p>Formulate a process for checking on the transparency of 3rd party providers on NPI</p> <p>Consider political briefings before the Project becomes a national venture</p> <p>Consult with the Privacy Commissioner when the Project goals are known, defined and accepted</p>
<p>Security</p>	<p>Create clear rules and process about access to NPI in VIBE</p> <p>Create a contractual relationship with SecuroGroup/Fusion that includes security requirements for VIBE</p> <p>Manage the relationships with 3rd party providers of NPI by establishing clear Police expectations of practices in collecting and managing personal information</p>
<p>Use of personal information</p>	<p>Establish rules and guidance about how NPI can be used by Police including the limits of use</p>
<p>Retention of personal information</p>	<p>Establish retention periods that are commensurate with the various uses or purposes for which NPI will be of value to Police</p>
<p>Governance and Assurance</p>	<p>Introduce responsibility for ongoing oversight of the Project to a National Police governance group</p> <p>Introduce a robust assurance reporting model that includes consideration of a truly independent 3rd line of defence</p>